FINAL REPORT

Policy Challenges for the Internet of Things:
Turning Opportunities into Realities

3rd Leipzig IOT Meeting in connection with the IGF Dynamic Coalition of the Internet of Things,
organized by Medienstadt Leipzig e.V.,
in co-operation with GS1, Tech America and the German Internet Economy Association (eco),
supported by VeriSign and Afilias

Marriott Hotel Leipzig, August, 2-3, 2013

1.   25 participants from 8 countries (Germany, Denmark, US, Netherlands, Belgium, China, Russia, Pakistan), representing stakeholders from government, private sector civil society and the technical community, participated in the 3rd Workshop of the IGF IOT Dynamic Coalition (IOT DC) on the Internet of Things in Leipzig, August 1 – 2, 2013.

2.   Based on an introductory report by Avri Doria, independent Internet consultant and former Chair of ICANN´s GNSO Council, who serves also since 2011 as one of the Interim Co-Chairs of the IOT DC, an intensive discussion covered a broad range of basic issues related to the ongoing IOT policy debate.

3.   The main three messages from the workshop, which took place under the Chatham House rules are
   a. There is a need to move forward by putting the opportunities for new innovative IOT services and applications into the center of the discussion. Specific policy issues as governance, privacy and security has to be discussed when they emerge as concrete problems of a specific service and should be managed, if needed, on a case by case basis.
   b. there is NO special IOT Governance. IOT is just another Internet application and should be managed and further developed under the general principles and norms for Internet Policy Making as laid down in various instruments adopted, inter alia, by the OECD or the Council of Europe. There is no need to have a new and specific institutional framework for IOT. The management and allocation of identifiers as IP addresses, domain names or numbers for RFID chips should be done within the framework of existing institutions as RIRs or according to transparent polices, adopted be the IOT service providers.
   c. there is a need for more outreach towards a global IOT discussion which goes beyond the EU and the US and should include big emerging Internet nations and regions as China, Brazil, Russia, India and Africa. The discussion should involve all stakeholders from government, private sector technical community and civil society/end-users. The IGF and its Dynamic IOT Coalition could be developed into the main space for such a discussion.

4.   The conclusions from the Workshop are summarized as below in form of the "IOT Messages from Leipzig". They will constitute the basis for discussions during the forthcoming Workshop on the Internet of Things at the 8th UN sponsored Internet Governance Forum (IGF) in Bali/Indonesia, October 21, 2013.

IOT Messages from Leipzig

1. *The Internet of Things is NOT a separated part of the Internet. IOT is just another application which offers object related services by using Internet protocols and infrastructure, including established routing, naming and numbering mechanisms. From an architectural perspective, IOT is the result of an evolutionary change of the Internet which leads to a seamless integration of overlaying and underlaying services.*
2. *While there is a need for further discussion to clarify the whole IOT concept, including it political, economic, social, cultural, legal and security implications, there is no need to work towards a global consensus on a "IOT definition" or am "IOT Organization".*
3. *Discussion on IOT policies should be "fact" and not "fear" based.*
4. *Whereas policy discussions in the past took place mainly on a regional level, in particular in Europe, there is a need to globalize the discussion. A useful platform for IOT policy discussion is the UN sponsored Internet Governance Forum (IGF) and its IOT Dynamic Coalition.*
5. *The development of new IOT Services is enabled by technological innovations, driven by user needs to improve the quality of live and implemented by market mechanisms. Insofar they include technical aspects, have to be based on a workable business model, are embedded into a general Internet Governance policy framework and have to match Human Rights standards.*
6. *IOT services and applications are closely linked to other categories of Internet based services emerging from M2M communications, cloud computing and the mobile Internet. IOT changes the traditional "value chain" into an innovative "value circle" where the commercial and non-commercial users are sitting in the driver´s seat.*
7. *IOT is a cross cultural, cross sectoral and cross stakeholder development which needs more interaction among the involved parties. So far, the various groups as the logistics and retailer industries, the technical developers and the Internet Governance constituencies have discussed the IOT issues mainly in isolated silos of their own communities. There is a need to go out of the silos, to build bridges and to enhance communication, coordination and collaboration among all groups which have a stake in the IOT development.*
8. *To enhance security and privacy in IOT services creative solutions in technology developments are needed. Build-in Security, privacy by design and strong end-to-end encryption can lead both to higher security, privacy protection and less misuse as well as to new business opportunities.*
9. *While IOT services are using existing Internet routing, naming and numbering mechanisms to identify the objects which are connected to the Internet and to enable Object-to-Object (O2O) and Object-to-Person (O2P) communication, there is neither a technical obligation to have a unique IOT naming or numbering space nor a political need to establish a global or regional coordination body for the allocation of IOT identifiers. Different IOT services can co-exist on a decentralized basis and its management can be delegated to various entities.*
10. *IOT is an opportunity for innovation, it is an invitation to investigate unchartered territories, it offers room for playing on an experimental basis and has the potential become an engine for economic growth and job creation.*
11. *Build in Security and Privacy standards in IOT services for enhanced human rights standards offers also new business opportunities. However, it is certainly problematic to introduce "pay for your right"-concepts where individuals have "to pay" to enjoy their constitutional rights. This could lead to new divisions within a democracy where*

individuals cannot make use of their fundamental rights because they can´t afford it and it is "too expensive" for them.

12. *Policy frameworks for IOT should allow enough flexibility for experimentation in "linking the dots". IOT Policies should be based more on monitoring and review mechanisms instead of hard law or legally binding treaties taking into account that technology moves faster than regulation.*

13. *IOT Services multiply the opportunities also for misuse and criminal activities. Counter strategies to enhance security and to build trust and confidence in IOT services needs the involvement and enhanced cooperation among all stakeholders from government, the private sector, the technical community as well as the civil society.*

14. *There is a high risk, that IOT developments can open technical opportunities which would allow the undermining of established civil and political rights and the rule of law which constitute the basis of a democratic society. An ubiquitous tracing and tracking of every individual via objects which can be linked to this person would violate the right to privacy which is a fundamental human rights, enshrined in Article 12 of the Universal Declaration of Human Rights (1948) and Article 17 of the International Covenant on Civil and Political Rights (1966).*

15. *Not everything what is technically possible is legal under the rule of law. There should be user options for "opt in" and opt out" for various services. A proposal was made to investigate the feasibility of drafting of a text for something like a universal "Hippocractic Oath" for IOT services based on the "do not harm" principle in the IOT space.*